

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of

YANG PENG ET AL.

Serial No.: 10/575,424

Filed: APRIL 10, 2006

Atty. Docket No.: 2003P00723WOUS

Confirmation No.: 3752

Examiner: JEFFREY D. POPHAM

Group Art Unit: 2491

Title: OPTICAL DISC, PLAYER FOR THE OPTICAL DISC AND ITS PLAY BACK
METHOD

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Sir:

Appellants herewith respectfully present its Brief on Appeal as follows:

REAL PARTY IN INTEREST

The real party in interest is Koninklijke Philips Electronics N.V., a corporation of The Netherlands having an office and a place of business at Groenewoudseweg 1, Eindhoven, Netherlands 5621 BA.

RELATED APPEALS AND INTERFERENCES

To the best of Appellants' knowledge and belief, there are no related appeals or interferences.

STATUS OF CLAIMS

Claims 17-32 are pending in this application. Claims 1-16 are canceled. Claims 17, 20 and 25 are independent claims. All pending claims are rejected in the Final Office Action that issued August 10, 2011. An Amendment After Final Office Action was filed on October 11, 2011 in response to the Final Office Action including amendments to the claims. The rejection was upheld in the Advisory Action mailed on October 24, 2011 that stated that the amendments to the claims would be entered for purposes of appeal. Accordingly, claims 17-32 as submitted in the Amendment After Final Office Action are the subject of this appeal.

STATUS OF AMENDMENTS

An Amendment was filed in response to the Final Office Action. This Appeal Brief is in response to the Final Office Action mailed on August 10, 2011, that finally rejected claims 17-32, which remain finally rejected in the Advisory Action mailed on October 24, 2011.

SUMMARY OF CLAIMED SUBJECT MATTER

The present invention, for example as claimed in claim 17 relates to an optical disk playing system having a plurality of downloadable external media content (e.g., see present application, page 5, lines 5-11) provided on one or more computing devices distributed on a network (e.g., see present application, page 5, lines 12-19), each downloadable external media content having been added with a private key (e.g., see present application, page 5, lines 12-19); an optical disk comprising internal media content associated with the external media content (e.g., see present application, page 5, lines 12-19) and a public key to verify the authenticity of each of the external media content (e.g., see present application, page 5, line 20 through page 6, line 14); an output for playing the internal media content in coordination with the associated authenticated external media content (e.g., see present application, page 7, lines 13-21), wherein the authenticity of the external media content is verified independent of the authenticity of the one or more computing devices on which the external media content is provided (e.g., see present application, page 5, line 20 through page 7, line 23).

The present invention, for example as claimed in claim 20, relates to an optical disk player having an optical disk driver unit to read-out internal media content (e.g., see present application, page 5, lines 12-19) and a public key (e.g., see present application, page 5, line 20 through page 6, line 14), both provided on a same optical disk, the public key is for authenticating external media content associated with the internal media content (e.g., see present application, page 5, line 20 through page 6, line 14); a network interface to

download one or more external media content (e.g., see present application, page 5, lines 5-11), each external media content having been added with a private key (e.g., see present application, page 5, lines 12-19) and is provided on one or more computing devices distributed on a network; a control system to verify the authenticity of the downloaded external media content using the public key read-out from the optical disk (e.g., see present application, page 5, line 20 through page 6, line 14); and an output portion to output the internal media content in coordination with the associated downloaded authenticated external media content (e.g., see present application, page 7, lines 13-21), wherein the authenticity of the external media content is verified independent of the authenticity of the one or more computing devices on which the external media content is provided (e.g., see present application, page 5, line 20 through page 7, line 23).

The present invention, for example as claimed in claim 25, relates to a method for playing an optical disk including reading-out internal media content (e.g., see present application, page 5, lines 12-19) and a public key, both provided on a same optical disk, the public key is to verify authenticity of external media content associated with the internal media content (e.g., see present application, page 5, line 20 through page 6, line 14); downloading from one or more computing devices distributed on a network (e.g., see present application, page 5, lines 12-19) one or more external media content (e.g., see present application, page 5, lines 5-11) having been added with a private key; verifying the authenticity of each of the downloaded external media content using the public key read-out from the optical disk (e.g., see present application, page 5, line 20 through page 6, line 14);

and outputting the internal media content in coordination with the one or more associated downloaded authenticated external media content (e.g., see present application, page 7, lines 13-21), wherein the authenticity of the external media content is verified independent of the authenticity of one or more computing devices on which the external media content is provided (e.g., see present application, page 5, line 20 through page 7, line 23).

It should be explicitly noted that it is not the Appellants' intention that the present invention be limited to operation within the illustrative recitations described above beyond what is required by the claim language. Further description of the illustrative device and method is provided above indicating portions of the claims which cover the illustrative device and method merely for compliance with requirements of this appeal without intending any further interpreted limitations be read into the claims as presented.

GROUND OF REJECTION TO BE REVIEWED ON APPEAL

Whether claims 17-18, 20, 22, 24-25, 27-29 and 31-32 of U.S. Patent Application Serial No. 10/575,424 are obvious under 35 U.S.C. §103(a) over U.S. Patent Publication No. 2004/0001697 to Kumbayashi ("Kumbayashi") in view of U.S. Patent No. 6,470,085 to Uranaka ("Uranaka").

Whether claim 19 of U.S. Patent Application Serial No. 10/575,424 is obvious under 35 U.S.C. §103(a) over Kumbayashi in view of Uranaka and further in view of U.S. Patent No. 5,754,648 to Ryan ("Ryan").

Whether claims 21 and 26 of U.S. Patent Application Serial No. 10/575,424 are obvious under 35 U.S.C. §103(a) over Kumbayashi in view of Uranaka and further in view of U.S. Patent Publication No. 2002/0073316 to Collins ("Collins").

Whether claims 23 and 30 of U.S. Patent Application Serial No. 10/575,424 are obvious under 35 U.S.C. §103(a) over Kumbayashi in view of Uranaka and further in view of U.S. Patent Publication No. 2004/0126095 to Tsumagari ("Tsumagari").

ARGUMENT

Claims 17-18, 20, 22, 24-25, 27-29 and 31-32 are said to be anticipated over Kumbayashi in view of Uranaka.

Appellants respectfully request the Board to address the patentability of independent claims 17, 20, and 25 and further claims 18-19, 21-24, and 25-32 as based on the requirements of the independent claims. This position is provided for the specific and stated purpose of simplifying the current issues on appeal. However, Appellants herein specifically reserve the right to argue and address the patentability of the dependent claims at a later date should the separately patentable subject matter of the dependent claims later become an issue. Accordingly, this limitation of the subject matter presented for appeal herein, specifically limited to discussions of the patentability of the independent claims is not intended as a waiver of Appellants' right to argue the patentability of the further claims and claim elements at that later time.

Kumbayashi is directed to a video reproduction apparatus including a playback engine for reproducing a DVD and an extension navigation "ENAV engine". Kumbayashi explains that ENAV contents 101 and DVD contents 102 are stored on a DVD 100 and ENAV contents 103 is provided via a server 7 on the Internet 6. Kumbayashi in paragraph [0239] states that the server that provides contents 103 stores a secret key S_k and the parser/interpreter 35 prestores a public key P_k corresponding to the server secret key S_k , for example, in a ROM area during manufacture. In other words, in Kumbayashi it is the parser/interpreter 35, which is an integral part of the video reproduction apparatus that

prestores the public key. Further, the prestoring is not on the DVD 100 having the ENAV and DVD contents 101, 102 that is being reproduced but instead on "a ROM area". Kumbayashi does not explain where the ROM area is located. Similarly, Kumbayashi does not limit the DVD 100 to being only ROM. Kumbayashi does not describe its DVD 100 as including the public key. Accordingly, it is respectfully submitted that Kumbayashi does not teach, disclose, or suggest "internal media content and a public key, both provided on a same optical disk, the public key is for authenticating external media content associated with the internal media content", as recited in claim 20, for example.

It is undisputed, as admitted at page 8 of the Final Office Action that Kumbayashi fails to disclose that the public key is provided and read from the same optical disk as the internal content. Uranaka is introduced for disclosing that which is admitted missing from Kumbayashi. However it is respectfully submitted that reliance on Uranaka is misplaced.

The Final Office Action references col. 6, lines 42-54; col. 7, lines 9-33; Col. 8, lines 23-41; and col. 12, lines 12-15 of Uranaka as showing the above quoted limitation admitted missing from Kumbayashi. The Applicants have addressed each of the referenced sections at length previously (see, Amendment mailed on October 11, 2011) and argued that Uranaka does not teach the public key on the same medium with the content. In short, at **col. 6, lines 42-54** Uranaka states that "[t]he IC card 5 stores a user's password PW_u and a user's secret key SK_u which corresponds to the user's public key PK_u ". This reference does not teach, disclose or suggest where the public key is stored. At **col. 7, lines 9-33** Uranaka does not discuss where the public key is stored and merely describes reading and

executing the volume control program 24 that prompts the user to select a desired one of the applications. The public key is discussed at col. 7, lines 1-9, but there "... he or she has to have the PK_u-encrypted version of an application-encrypting key (K_v) recorded in the burst cutting area of the desired DVD 3 by notifying his or her public key PK_u which corresponds to his or her secret key SK_u stored in the IC card 5." This however does not teach, disclose or suggest "internal media content and a public key, both provided on a same optical disk, the public key is for authenticating external media content associated with the internal media content".

Where at cols. 6 and 7 Uranaka discusses user's public key PK_u, at **col. 8, lines 23-41** Uranaka describes a table 75 used for "associating the server public key (PK_s) contained in the distribution descriptor 23 recorded in the burst cutting area of the DVD with the ID and the network address". The Examiner argues that it is enough to have any public key to be read from the DVD (see, Final Office Action, page 4). However, here an item being stored has a similar name, yet does not perform or teach performance of the function recited in the claims. This argument is supported at col. 12, lines 12-15 of Uranaka which describes encrypting with a server public key read from the distribution descriptor 23 recorded in the burst cutting area of the DVD. Accordingly, contrary to the claims, Uranaka teaches using the public key (PK_s) stored in the DVD for encrypting NOT for "authenticating external media content", as recited in the claims of the present application. Storing of "public key" that has no relation to the content stored on the DVD or to the related content stored elsewhere and moreover used to encrypt does not teach "internal media content and a public key, both

provided on a same optical disk, the public key is for authenticating external media content associated with the internal media content", as recited in claim 20, for example.

For the reasons discussed immediately above Kumbayashi in view of Uranaka, Ryan, Collins, and Tsumagari does not make the claims obvious.

The Advisory Action, maintains the rejections of the Final Office Action. This position is traversed.

First, the advisory Action states that "Applicant argues that Kambayashi does not teach the public key being stored on the DVD. As Uranaka was used in rejecting this limitation, this argument is moot." This statement is not understood. Appellants have accepted this position admitted at page 8 of the Final Office Action as "undisputed". The Examiner then repeats the above argued issues, for example, that it is enough to have any public key to be read from the DVD. Appellants' position on this point is argued above. Appellants remind the Examiner that the claims recite verifying the authenticity of "the downloaded external media content using the public key read-out from the optical disk" not of the server hosting the external media content. As explained in the specification, "the contents are stored in the web sever directly without authentication". Therefore, authenticating the server, as in the prior art, does not authenticate the content.

The Advisory Action's takes a position that "Kambayashi discloses use of a server public key to authenticate data downloaded from the server", that "Uranaka discloses storing this server public key on the DVD together with the content" and the server public key of Uranaka corresponds to the server public key of Kambayashi the server public key in

each of Kambayashi and Uranaka can be seen as the public key of the claims. It is respectfully submitted that this position, in view of Appellants arguments presented above with support from the specification and the citations to the prior art references themselves, has no merit.

It is respectfully submitted that Kumbayashi in view of Uranaka does not teach, disclose or suggest, amongst other patentable elements, (illustrative emphasis provided) "an optical disk driver unit to read-out internal media content and a public key, both provided on a same optical disk, the public key is for authenticating external media content associated with the internal media content; a network interface to download one or more external media content, each external media content having been added with a private key and is provided on one or more computing devices distributed on a network; a control system to verify the authenticity of the downloaded external media content using the public key read-out from the optical disk; and an output portion to output the internal media content in coordination with the associated downloaded authenticated external media content, wherein the authenticity of the external media content is verified independent of the authenticity of the one or more computing devices on which the external media content is provided", as recited in claim 20 and as similarly recited in claims 17 and 25.

Based on the foregoing, the Appellants respectfully submit that independent claims are patentable and notice to this effect is earnestly solicited. The dependent claims respectively depend from one of the independent claims and accordingly, are allowable for at least this reason as well as for the separately patentable elements contained in each of

said claims. Accordingly, separate consideration of each of the dependent claims is respectfully requested.

In addition, Appellants deny any statement, position, or averment of the Examiner that is not specifically addressed by the foregoing argument and response. Any rejections and/or points of argument not addressed would appear to be moot in view of the presented remarks. However, the Appellants reserve the right to submit further arguments in support of the above stated position, should that become necessary. No arguments are waived and none of the Examiner's statements are conceded.

Claim 19 is said to be anticipated over Kumbayashi in view of Uranaka and Ryan.

Ryan is cited for allegedly showing elements of the dependent claims yet does not cure the deficiencies in each of Kumbayashi and Uranaka. Accordingly, it is respectfully submitted that claim 19 is allowable at least based on dependence from the independent claims.

Claims 21 and 26 are said to be anticipated over Kumbayashi in view of Uranaka and Collins.

Collins is cited for allegedly showing elements of the dependent claims yet does not cure the deficiencies in each of Kumbayashi and Uranaka. Accordingly, it is respectfully submitted that claims 21 and 26 are allowable at least based on dependence from the independent claims.

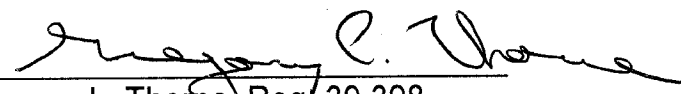
Claims 23 and 30 are said to be anticipated over Kumbayashi in view of Uranaka and Tsumagari.

Tsumagari is cited for allegedly showing elements of the dependent claims yet does not cure the deficiencies in each of Kumbayashi and Uranaka. Accordingly, it is respectfully submitted that claims 23 and 30 are allowable at least based on dependence from the independent claims.

CONCLUSION

Claims 17-32 are patentable over the presented prior art references. Thus the rejection of the claims should be reversed.

Respectfully submitted,

By 
Gregory L. Thorne, Reg. 39,398
Attorney for Appellants
January 3, 2012

THORNE & HALAJIAN, LLP

111 West Main Street
Bay Shore, NY 11706
Tel: (631) 665-5139
Fax: (631) 665-5101

APPENDIX A

CLAIMS ON APPEAL

Listing of Claims:

1-16. (Canceled)

17. (Previously presented) An optical disk playing system comprising:

a plurality of downloadable external media content provided on one or more computing devices distributed on a network, each downloadable external media content having been added with a private key;

an optical disk comprising internal media content associated with the external media content and a public key to verify the authenticity of each of the external media content;

an output for playing the internal media content in coordination with the associated authenticated external media content,

wherein the authenticity of the external media content is verified independent of the authenticity of the one or more computing devices on which the external media content is provided.

18. (Previously presented) The optical disk playing system according to claim 17, wherein the public key is stored in a BCA (Burst Cutting Area) zone of the optical disk.

19. (Previously presented) The optical disk playing system according to claim 17, wherein the public key is stored in a media content zone of the optical disk.

20. (Previously presented) An optical disk player comprising:

an optical disk driver unit to read-out internal media content and a public key, both provided on a same optical disk, the public key is for authenticating external media content associated with the internal media content;

a network interface to download one or more external media content, each external media content having been added with a private key and is provided on one or more computing devices distributed on a network;

a control system to verify the authenticity of the downloaded external media content using the public key read-out from the optical disk; and

an output portion to output the internal media content in coordination with the associated downloaded authenticated external media content,

wherein the authenticity of the external media content is verified independent of the authenticity of the one or more computing devices on which the external media content is provided.

21. (Previously presented) The optical disk player according to claim 20, wherein the control system detects whether the downloaded external media content is integral before

verification, wherein said verification will not be executed if the downloaded external media content is detected to not be integral.

22. (Previously presented) The optical disk player according to claim 20, wherein the downloaded external media content is an application program.

23. (Previously presented) The optical disk player according to claim 22, wherein the application program is a JAVA language application program.

24. (Previously presented) The optical disk player according to claim 20, wherein the control system verifies the authenticity of the downloaded external media content by performing asymmetric cryptography using the public key stored on the optical disk corresponding to the private key of the downloaded external media content.

25. (Previously presented) A method for playing an optical disk, comprising acts of:

reading-out internal media content and a public key, both provided on a same optical disk, the public key is to verify authenticity of external media content associated with the internal media content;

downloading from one or more computing devices distributed on a network one or more external media content having been added with a private key;

verifying the authenticity of each of the downloaded external media content using the public key read-out from the optical disk; and

outputting the internal media content in coordination with the one or more associated downloaded authenticated external media content,

wherein the authenticity of the external media content is verified independent of the authenticity of one or more computing devices on which the external media content is provided.

26. (Previously presented) The method according to claim 25, further comprising acts of:

detecting if the downloaded external media content is integral; and

executing the verifying act only if the downloaded external media content is detected to be integral.

27. (Previously presented) The method according to claim 25, wherein the coordination between the read-out internal media content and the downloaded external media content will not be established if the downloaded external media content is not authenticated.

28. (Previously presented) The method according to claim 27, wherein the coordination between the read-out internal media content and downloaded external media content will be established if the downloaded external media content is authenticated.

29. (Previously presented) The method according to claim 25, wherein the downloaded external media content is an application program.

30. (Previously presented) The method according to claim 29, wherein the application program is a JAVA language application program.

31. (Previously presented) The method according to claim 25, wherein verifying the authenticity of the downloaded external media content comprises an act of performing asymmetric cryptography using the public key read-out from the optical disk corresponding to the private key of the downloaded external media content.

32. (Previously presented) The method according to claim 25, wherein the optical disk comprises digital information stored thereon, the stored digital information comprising network address information that is used to download the external media content and the public key that is used to verify the authenticity of the downloaded external media content before playing the internal media content in coordination with the external media content.

APPENDIX B

Evidence on Appeal

None

APPENDIX C

Related Proceedings of Appeal

None